Cybernetics and Systems Analysis, Vol. 42, No. 3, 2006

CYBERNETICS

STATEMENT AND SOLUTION OF SOME PROBLEMS ON A MATHEMATICAL SAFE

G. A. Donets[a] **and Bin Zhan**[b]

UDC 510.1

The problem on a mathematical safe is formulated and studied in terms of graph theory. The cases of simplest digraphs such as paths, contours, and doubly connected components are analyzed. A number of statements on the existence of solutions to these problems are proved. The results obtained are extended to the case of corresponding nondirected graphs.

Keywords: *mathematical safe, set of locks, dependency matrix of locks, solution of a system of equations, final state of a safe, residue class.*

INTRODUCTION

The general problem on a mathematical safe was first formulated in [1].

Problem. A mathematical safe is understood to be a system $S(\mathbf{Z}, \mathbf{b}, \langle \mathbf{Z} \rangle)$ that consists of a set of locks $\mathbf{Z} = \{z_1, z_2, \ldots, z_n\}$, the vector of states of the safe $\mathbf{b} = (b_1, b_2, \ldots, b_n)$, where $b_i \in \{0, 1, \ldots, k_i - 1\}$ is the state of the ith lock, and a set $\langle \mathbf{Z} \rangle = \{Z_1, Z_2, \ldots, Z_n\}$, $z_l \notin Z_l$, $Z_l \in 2^{\mathbf{Z}}$ $(1 \le i, l \le n)$. As a result of one clockwise turn of the key in the lth lock z_l, all the locks $z_j \in Z_l$ pass from the jth state b_j to the state $(b_j + 1) (\mathrm{mod} k_j)$. The safe is considered to be open if it is in the state $\mathbf{b} = (0, 0, \ldots, 0) = \mathbf{b}_{\mathrm{fin}}$. For each lock z_j, it is necessary to find the number of turns x_j of the key that allow one to open the safe.

We call a vector $\mathbf{X} = (x_1, x_2, \ldots, x_n)$ a solution to the problem on a safe. We call the set $\langle \mathbf{Z} \rangle$ an incidence set. It can be written in the form of an incidence matrix $\mathbf{A}_0 = a_{ij}^0$ of size $n \times n$ in which the main diagonal consists of zeros and $a_{ij}^0 = 1$ if z_j belongs to a set Z_i $(1 \le i,\ j \le n)$ and equals zero in the opposite case. We assign to the matrix $\mathbf{A}_0$ a directed graph $G(\mathbf{Z})$ in which an outgoing edge of a node z_i is an incoming edge of a node z_j when $a_{ij}^0 = 1$. Depending on the complexity of a given matrix, various problems on a mathematical safe arise. We denote $\mathbf{A} = \mathbf{A}_0 + \mathbf{E}_n$, where $\mathbf{E}_n$ is an identity matrix. Then the general problem on a safe is reduced to the solution of the following system of linear congruences:

$$\mathbf{X}\bar{\mathbf{a}}_i + b_i \equiv 0 (\mathrm{mod}\, k_i)\ (1 \le i \le n), \tag{1}$$

where $\bar{\mathbf{a}}_i$ is the ith column of the matrix $\mathbf{A}$.

The initial state of the safe $\mathbf{b}$ is assumed to be known or at least it can be easily computed. If we have $k_i = \mathbf{K} = \mathrm{const}$ for all $1 \le i \le n$, then such locks are called the locks of the same type.

SOLUTION OF THE PROBLEM FOR SIMPLEST GRAPHS

Let us consider the problem with locks of the same type for the most simple case when $\mathbf{K} = 2$, i.e., $b_i \in \{0, 1\}$ $(1 \le i \le n)$. Let, in the directed graph $G(\mathbf{Z})$ corresponding to the matrix $\mathbf{A}_0$, $d^+(z)$ and $d^-(z)$ denote the number

---

[a]Cybernetics Institute, National Academy of Sciences of Ukraine, Kiev, Ukraine. [b]National Technical University "Kiev Polytechnic Institute," Kiev, Ukraine. Translated from Kibernetika i Sistemnyi Analiz, No. 3, pp. 3-14, May-June 2006. Original article submitted January 16, 2006.

1060-0396/06/4203-0311

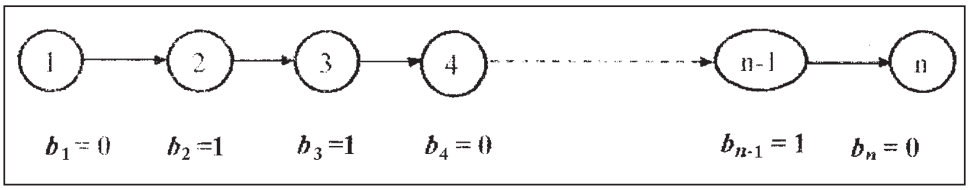

Fig. 1. A safe specified in the form of a path.

of outgoing and incoming edges of a node z. Then the degree of the node z is $d(z) = d^+(z) + d^-(z)$. If we have $d^+(z) = d^-(z) = 0$ for all the nodes of the graph, which is equivalent to $\langle \mathbf{Z} \rangle = \varnothing$, then all the locks are isolated and the problem is solved for each lock irrespective of the others. Therefore, we will assume that the inequality $d(z_i) \geq 1$ is always true for all $i = 1, 2, \ldots, n$. The case when $d(z_i) = 1$ represents all possible matchings of locks, and its solution is of no interest in view of its unambiguity. Let us consider the constraint $d(z_i) \leq 2$.

In this case, the corresponding graph consists of several components of two types, namely, a chain or a cycle with arbitrarily oriented edges. We will find solutions for each component independently.

Let several nodes of the graph being considered form a chain in which all the edges are oriented in one direction, i.e., the chain forms a path (Fig. 1).

Let us number its nodes from 1 up to n, starting from the node that has no incoming edge. The numbers of nodes are specified in bubbles and the states of locks (nodes) are shown below the bubbles.

We put $i = 1$. If $b_i = 0$, then we pass to the node $i + 1$. If $b_i = 1$, then we turn the ith lock z_i to set it to zero and b_{i+1} is set to the state $(b_{i+1} + 1) \pmod 2$. We pass to the $(i + 1)$th node. As a result, we arrive at the node n whose state is set to zero, $b_n = 0$. Hence, for the entire component, we obtain states $b_i = 0 (1 \leq i \leq n)$. The number of executed operations (turns of the key) can be calculated. In the vector $\mathbf{b}$, we select the components consisting of contiguous unities. We denote the totality of components that contain α unities by $I(\alpha)$. Similarly, we denote by $o(\beta)$ the totality of components of the vector $\mathbf{b}$ that contain β contiguous zeros. Then $\mathbf{b}$ splits into disjoint sets

$$\mathbf{b} \sim \{I(\alpha_1), o(\beta_1), I(\alpha_2), o(\beta_2), \ldots, I(\alpha_s), o(\beta_s)\}, \tag{2}$$

where $I(\alpha_i)$ and $o(\beta_s)$ can be empty.

Let

$$\sum_{i=1}^{r} |I(\alpha_i)| = \lambda(1). \tag{3}$$

In representation (2), we select the sets $I(\alpha_i)$ for which we have $\alpha_i \equiv 0 \pmod 2$. It is obvious that, after execution of $\frac{\alpha_i}{2}$ operations, these states can be set to zero.

We eliminate all such subsets from set (2) and unite their neighboring nullity sets. The sets remain that contain only an odd number of unities α_j $(j = 0, 1, \ldots)$. With the help of $\frac{\alpha_j - 1}{2}$ operations, we can provide the transition of $\alpha_j - 1$ locks to the state 0. We eliminate these states from (2), and renumber the remaining sets (we denote them by one letter) that contain only one unity as follows:

$$\{I_1, o(\gamma_1), I_2, o(\gamma_2), \ldots, I_l, o(\gamma_l)\} \quad (l \leq s). \tag{4}$$

Here, I_1, $\bigcup_{i=1}^{l} \mathbf{I}_j$, or $o(\gamma_l)$ can be empty. Beginning with the unity of I_1 and ending with the unity of I_2, we set all the states to 0 using $o(\gamma_1) + 1$ operations. Then we analogously transform the set of states beginning with I_3 and ending with I_4, etc. If $l \equiv 0 \pmod 2$, then the process terminates at the unity of I_l. If we have $l \equiv 1 \pmod 2$, then, beginning with I_l and ending with the node n, inclusively, we set all the locks to the state 0. This is equivalent to the fact that there exists the fictitious lock $(n + 1)$ for which we have

$$b_{n+1} = 1 = I_{l+1}.$$

In any case, the total number of operations is equal to

$$\left\lfloor \frac{\lambda(1) + 1}{2} \right\rfloor + \sum_{i=1}^{\left\lfloor \frac{l+1}{2} \right\rfloor} \left| o(\gamma_{2i-1}) \right|.$$

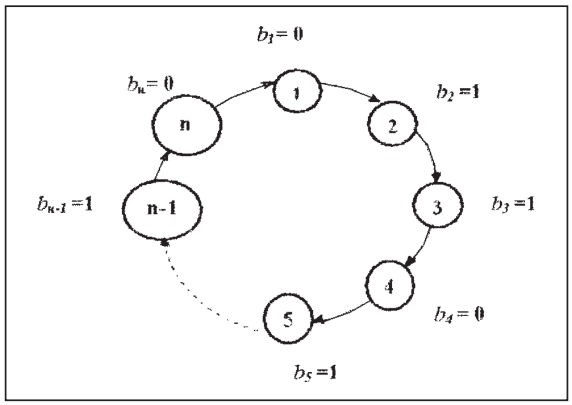

Fig. 2. A safe specified in the form of a contour.

Chains with arbitrarily directed edges form a collection of paths whose orientations alternate. Common nodes of two paths have the degree $d^+(i) = 2$ or $d^-(i) = 2$ in turn. We begin switching operations with the nodes of degree $d^+(i) = 2$ and gradually set the nodes of the entire chain to the state 0.

Let us consider cycles. If their edges are not unidirectional, then a component is formed by a composition of several paths and the problem is solved in the same way as for chains, starting from the nodes i of degree $d^+(i) = 2$.

We have a special case when a cycle is a contour. We number its nodes from 1 to n (Fig. 2).

LEMMA 1. In order that the problem on a safe for a contour of length n have a solution, it is necessary and sufficient that

$$\sum_{i-1}^{n} b_i \equiv 0 (\mathrm{mod}\ 2). \tag{5}$$

To prove the lemma, we write system (1) for the contour depicted in Fig. 2 as follows:

$$\left.\begin{array}{rcccccccc} x_1 & + & . & . & . & . & . & + x_n & \equiv b_1 \\ x_1 & + & x_2 & . & . & . & . & . & \equiv b_2 \\ & & x_2 & + & x_3 & . & . & . & \equiv b_3 \\ & & & & x_3 & + & x_4 & . & \equiv b_4 \\ & & & & & . & . & . & . \\ & & & & & & & x_{n-1} + x_n & \equiv b_n \end{array}\right\} \mathrm{mod}\ 2. \tag{6}$$

Summing all the equalities of system (6), we obtain the necessity. In the left side, we obtain $0 (\mathrm{mod}\ 2)$ and, in the right side, we obtain the left side of equality (5). Let us assume that condition (5) is true. We will show how to set all the nodes of the contour to the state 0. If all $b_i = 1$ $(1 \le i \le n)$, then equality (5) implies the equality $n \equiv 0 (\mathrm{mod}\ 2)$. Then the states of all the nodes are set to 0 in $\frac{n}{2}$ operations. If there exists some $b_j = 0 (1 \le j \le n)$, then we eliminate the outgoing edge of the jth node. Renumbering the nodes as follows: $j+1 \to 1$, $j+2 \to 2$, etc., we obtain the path presented in Fig. 1. By virtue of condition (5), the number of sequences with odd numbers of unities in the path is even and, hence, after executing the corresponding operations, we obtain set (4) for which we have $l \equiv 0 (\mathrm{mod}\ 2)$. In this case, the transition $\mathbf{b} \to \mathbf{b}_{\mathrm{fin}}$ is realized without changing the state of the node n, which testifies to the truth of the lemma.

Note that if the inequality $l > 0$ is true, then there exist two methods of solution of the problem. In contrast to the above-mentioned node j, we find another node u such that an odd number of nodes that are in the state 1 will be between them. This is possible since we have $l \ge 2$. After executing all the corresponding operations, we obtain sets of the type of set (4) in the form

$$\{o(\gamma_1''),\ I_2, o(\gamma_2), I_3, \ldots, I_l\ o(\gamma_l), I_1, o(\gamma_1')\},$$

where $o(\gamma_1') + o(\gamma_1'') = o(\gamma_1)$.

In the first case, unity from I_1 is first chosen and the number of operations is equal to $p_1 = \frac{\lambda(1)}{2} + \sum_{i=1}^{l/2} |o(\gamma_{2i-1})$ and,

in the second case, I_2 is chosen and the number of operations equals $p_2 = \frac{\lambda(1)}{2} + \sum_{i=1}^{l/2} |o(\gamma_{2i})$. We choose $\min(p_1, p_2)$ in

the capacity of the optimal solution of the problem.

THE PROBLEM FOR GRAPHS WITH $d(z_i) \geq 3$

In this case, graphs form a more complex structure. The simplest structure among them is a transport network i.e., a directed graph that does not contain contours. Let us consider an arbitrary network without constraints on the degrees of nodes.

THEOREM 1. The problem on a safe formulated on a transport network always has a solution for an arbitrary initial state.

To prove the theorem, we first define the rank of each node by induction. We assign the rank $r(i) = 0$ to all the nodes without incoming edges. These nodes are called the sources of the network.

If there exists a set of nodes of rank $p-1 (p \geq 1)$ and also nodes of undefined rank, then we assign a rank p to all the sources of the network obtained after elimination of the nodes of rank $p-1$ together with their outgoing edges. The nodes that have no outgoing edges are called the drains of the network.

The proposed algorithm of solution of the problem consists of sequential switching of the locks (nodes) that are in the state 1 in ascending order of their ranks. The sequence of nodes of the same rank is arbitrary. The algorithm comes to an end when all the drains of the network assume the state 0.

Next in order of complexity is a structure consisting of several nonintersecting (independent) contours embedded into a network. It is suggested that if each contour is folded into one node, then we obtain an ordinary network without contours. One should take into account that each contour must not contain diagonals in the form of paths since, in this case, it would represent the union of contours that have common parts.

When the above algorithm processes the network, the zeroth-rank nodes, the first-rank nodes, etc. are successively set to the zero state. All such nodes together with their outgoing edges can be eliminated without influencing the solution of the problem.

Let us consider some contour C and select the set of nodes $\mu(C)$ from which at least one node of this contour is accessible. If, during some steps, all the nodes are set to the zero state, then we call the state of the contour C obtained as a result of these operations its canonical state.

THEOREM 2. The problem on a safe defined on a directed graph with independent contours has a solution for an arbitrary initial state if the canonical state of each contour satisfies condition (5).

Proof. We fold each contour C_i $(i \geq 1)$ into a node with the same designation. As a result, we obtain a network without contours. In order to solve the problem, we can use the same algorithm as in the proof of Theorem 1. In this case, a node C_j (a contour) is considered to be processed if the states of all the nodes of the contour are equal. When the algorithm passes to the jth contour (node) C_j of the least rank, all the nodes from which the nodes of C_j are reachable are already in the state 0. Consequently, the contour C_j is in the canonical state and all the reachable nodes can be eliminated together with their outgoing edges without influencing the solution of the problem. As a result, the nodes of the contour have incoming edges only from other nodes of the contour and arbitrary outgoing nodes. The system of congruences (1) written for the contour in the canonical state is of the form (6), which implies the necessity of the truth of conditions (5). Gradually setting other contours to the canonical state, we obtain a similar result for them, which testifies to the truth of the theorem.

The structures of the third type consist of collections of several intersecting contours embedded into a network. We call such a collection a doubly connected component. A contour is the simplest doubly connected component. As is obvious, to solve the problem defined on such a graph, one can use the above algorithm if doubly connected components are folded into nodes. However, though the solution is almost obvious for individual contours when condition (5) is true, it presents a definite difficulty for arbitrary doubly connected components. Let us consider some special cases.

For two intersecting contours, the solution is reduced to the performance of some standard actions (Fig. 3).

We distinguish between the common part of the component C_c (the nodes from 1 to k), the left part of the component C_{left} (the nodes from $k+1$ to $k+l$), and the right part C_r (the nodes from $k+l+1$ to n). If the number of nonzero states of

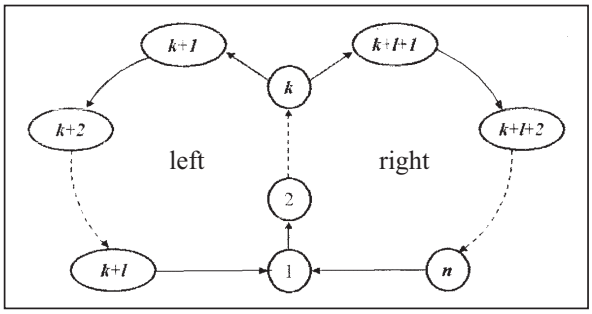

Fig. 3. A safe in the form of two contours.

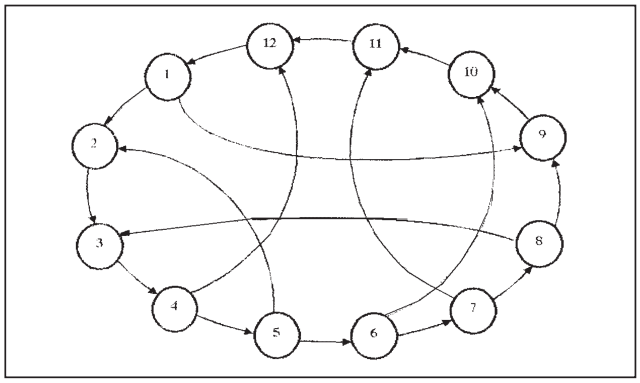

Fig. 4. The safe specified in the form of a contour with diagonals.

nodes of some part is greater than 1, then they can be easily bring to 0 or 1 by sequential switching (moving). We denote their number by $\lambda(C_{\mathrm{c}})$, $\lambda(C_{\mathrm{left}})$, and $\lambda(C_{\mathrm{r}})$; in this case, their values belong to the set {0, 1}. The combinations listed below are possible.

1. $\lambda(C_{\mathrm{left}})=\lambda(C_{\mathrm{r}})=1;\ \lambda(C_{\mathrm{c}})=0$.

We move the left unity to node 1 and the right unity to node *n*. Then we switch the node *n* and obtain zero states in the entire graph.

2. $\lambda(C_{\mathrm{left}})=\lambda(C_{\mathrm{r}})=0;\ \lambda(C_{\mathrm{c}})=1$.

We move unity to the node *k* and switch it. We obtain case 1.

3. $\lambda(C_{\mathrm{c}})=\lambda(C_{\mathrm{r}})=1;\ \lambda(C_{\mathrm{left}})=0$.

We move the right unity through node 1 and obtain two unities in C_{o} that can be simultaneously set to zeros.

4. $\lambda(C_{\mathrm{c}})=\lambda(C_{\mathrm{r}})=0;\ \lambda(C_{\mathrm{left}})=1$.

We switch the node *k* and obtain case 3. Let us consider a more sophisticated example presented in Fig. 4. The graph consists of one Hamiltonian circuit that includes all the nodes and edges connecting pairs of nodes of this contour.

If this graph contains nodes of degree 2, then such a node together with its incident edges can be replaced by one edge of the same orientation, which does not affect the solution of the problem. In this case, if the state of a node is equal to 1, then we move it to the next node. As a result of such operations, we obtain a regular graph of degree 3 with an even number of nodes. Each diagonal edge (i, j) uniquely determines a subcontour consisting of some subset of nodes. We denote such subcontours by $C(i, j)$. Let $\mu[C\{i, j)]$ denote the set of incoming edges of a subcontour $C(i, j)$, i.e., the edges in which only the final node belongs to the subcontour. We call edges $(u, v), (t, w) \in \mu[C(i, j)]$ conjugate if there exists a path that connects nodes *u* and *t* of outdegree 2 and any outgoing edge does not belong to $\mu[C(i, j)]$. In Fig. 4, the following edges are shown: (7,11) and (6,10), (7,11) and (8,9), and (4,2) and (6,10).

THEOREM 3. The system of equations (1) specifying a regular graph whose degree equals 3 and that consists of a Hamilton circuit with diagonals is dependent if and only if its subcircuit can be found with an even number of incoming edges that can be divided into conjugated pairs.

Proof. System (1) is linearly dependent if, in the matrix **A**, rows can be found whose sum is identically equal to $0 (\mathrm{mod}\ 2)$. If rows are taken that do not correspond to all the nodes of some subcontour, then they are never dependent since the number of variables always is greater than the number of rows in them. Therefore, the rows should be chosen that correspond to one of subcontours. In this case, an incoming edge of this subcontour can be necessarily found. By one of such edges for a subcontour $C(i, j)$ is $(j-1, j)$. Therefore, the *j*th row of the matrix **A** contains the variable x_{j-1}. If there is an edge (u, v) conjugated to the edge $(j-1, j)$, then we add the rows that correspond to the nodes of the path connecting the nodes *u* and *j*, except for the node *u*. The number of occurrences of all the variables that correspond to the nodes of a subcontour in system (1) is even and, hence, the sum of rows in these columns is equal to $0 (\mathrm{mod}\ 2)$. The number of occurrences of the variables corresponding to conjugated edges, except for the node *u*, is also even, and their sum is equal to $0 (\mathrm{mod}\ 2)$. By virtue of the conjugacy condition, edges of other variables do not belong to the path, which testifies to the truth of the theorem.

In the above example, let us consider the subcontour $C(1, 9)$. It contains the following four edges: (4, 12), (6, 10), (7, 11), and (8, 9). They can be divided into the following two pairs of conjugated edges: (4, 12), (6, 10) and (7, 11), (8, 9). We write the system of equations (1) for the entire subcontour and for the nodes of the paths connecting conjugated edges, except for nodes 4 and 7, in the form

$$\left.\begin{array}{cccccccccccccccccccccc}
x_1 & + & . & & . & & . & & . & & . & & . & & . & & . & + & x_{12} & \equiv & b_1 \\
 & & . & & . & & . & & . & & . & & . & & . & & . & & & & \\
. & & x_4 & + & x_5 & + & . & & . & & . & & . & & . & & . & & . & \equiv & b_5 \\
. & & . & & x_5 & + & x_6 & + & . & & . & & . & & . & & . & & . & \equiv & b_6 \\
. & & . & & . & & . & & x_7 & + & x_8 & + & . & & . & & . & & . & \equiv & b_8 \\
x_1 & + & . & & . & & . & & . & + & x_8 & + & x_9 & & . & & . & & . & \equiv & b_9 \\
. & & . & & . & & x_6 & + & . & & . & + & x_9 & + & x_{10} & & . & & . & \equiv & b_{10} \\
. & & . & & . & & . & & x_7 & + & . & & . & + & x_{10} & + & x_{11} & & . & \equiv & b_{11} \\
. & & x_4 & + & . & & . & & . & & . & & . & & . & + & x_{11} & + & x_{12} & \equiv & b_{12}
\end{array}\right\} \mod 2 .$$

The summation of all these equations gives the following result:

$$b_1 + b_5 + b_6 + b_8 + b_9 + b_{10} + b_{11} + b_{12} \equiv 0 (\mathrm{mod}\ 2) .$$

If the initial state of the safe does not satisfy this condition, then the problem has no solution.

THE PROBLEM DEFINED ON UNDIRECTED GRAPHS

If the graph on which the problem on a safe is stated is undirected, then the number of dependent locks increases. This problem can be reduced to a directed graph if each edge is replaced by two oppositely directed edges, but this only complicates the solution of the problem. On the other hand, the adjacency matrix of such graphs is symmetric, which simplifies the solution of the problem in some cases. For locks of the same type, system (1) can be rewritten in the form

$$\mathbf{A}\mathbf{X}^{\mathrm{T}} + \mathbf{b}^{\mathrm{T}} \equiv \mathbf{O} (\mathrm{mod}\ \mathbf{K}) . \tag{7}$$

We first consider a graph in the form of a chain. In contrast to system (6) composed for the path in which each row (except for the first and last ones) contains two variables, each row is longer by one variable for a chain in system (7). We write the following system for the chain with $n = 8$:

$$\left.\begin{array}{cccccccccccccccc}
x_1 & + & x_2 & + & . & & . & & . & & . & & . & & . & \equiv b_1 \\
x_1 & + & x_2 & + & x_3 & + & . & & . & & . & & . & & . & \equiv b_2 \\
. & & x_2 & + & x_3 & + & x_4 & + & . & & . & & . & & . & \equiv b_3 \\
. & & . & & x_3 & + & x_4 & + & x_5 & + & . & & . & & . & \equiv b_4 \\
. & & . & & . & & x_4 & + & x_5 & + & x_6 & + & . & & . & \equiv b_5 \\
. & & . & & . & & . & & x_5 & + & x_6 & + & x_7 & + & . & \equiv b_6 \\
. & & . & & . & & . & & . & & x_6 & + & x_7 & + & x_8 & \equiv b_7 \\
. & & . & & . & & . & & . & & . & & x_7 & + & x_8 & \equiv b_8
\end{array}\right\} \mod 2 . \tag{8}$$

LEMMA 2. The system of equations (8) that specifies an undirected chain is linearly dependent only for $n \equiv -1 (\mathrm{mod}\ 3)$.

Summing the first and second equations, we obtain $x_3 \equiv (b_1 + b_2) (\mathrm{mod}\ 2)$. We add the fourth and fifth equations to this result and obtain $x_6 \equiv (b_1 + b_2 + b_4 + b_5) (\mathrm{mod}\ 2)$. Continuing this process, we obtain the final value for x_{3l}, where

$l = \left\lfloor \frac{n}{3} \right\rfloor$. If $n = 3l - 1$, then we have $x_{3l} = 0$ since such a variable is absent. As a result, for $n \equiv -1 (\mathrm{mod}\ 3)$, we obtain the condition

$$\sum_{i=1}^{l} (b_{3i-2} + b_{3i-1}) \equiv 0 (\mathrm{mod}\ 2), \tag{9}$$

where $l = \frac{n+1}{3}$. This testifies to the linear dependence of system (8). If condition (9) is not true, then system (8) has no solution. One of the simplest examples of nonfulfilment of condition (9) is the state $\mathbf{b} = (0, 0, 0, 0, 0, 0, 0, 1)$ for which there exists no solution. This seemingly elementary result is in fact not quite obvious. For $n = 7$, the problem with the same state $\mathbf{b} = (0, 0, 0, 0, 0, 0, 0, 1)$ has a solution though it is not easy to find it. Let us consider the following successive steps of solution in which the lock being switched at each step is underlined:

$$(\underline{0}, 0, 0, 0, 0, 0, 1) \to (1, \underline{1}, 0, 0, 0, 0, 1) \to (0, 0, 1, \underline{0}, 0, 0, 1)$$

$$\to (0, 0, 0, 1, \underline{1}, 0, 1) \to (0, 0, 0, 0, 0, 1, \underline{1}) \to (0, 0, 0, 0, 0, 0, 0).$$

THEOREM 4. If we have $n \not\equiv -1 (\mathrm{mod}\ 3)$, then the solution of the problem on a safe defined on an undirected chain is as follows:

$$\begin{gathered} x_\alpha \equiv \sum_{i=1}^{l} (b_{3i-2} + b_{3i-1}) (\mathrm{mod}\ 2),\ \alpha \equiv 0 (\mathrm{mod}\ 3);\ l = \frac{\alpha}{3}; \\ x_\alpha \equiv \sum_{i=0}^{l} (b_{\alpha+3i+1} + b_{\alpha+3i+2}) (\mathrm{mod}\ 2),\ \alpha \equiv (n-2) (\mathrm{mod}\ 3);\ l = \frac{n-2-\alpha}{3}; \\ x_\alpha \equiv (x_{\alpha-1} + b_\alpha + x_{\alpha+1}) (\mathrm{mod}\ 2),\ x_0 = x_{n+1} = 0;\ \alpha \equiv (n-1) (\mathrm{mod}\ 3). \end{gathered} \tag{10}$$

Proof. The first solution for $\alpha \equiv 0 (\mathrm{mod}\ 3)$ has been obtained in proving Lemma 2. The second solution is similarly obtained if we begin the execution of the same operations with the last and penultimate rows of system (8). As a result, we have the solution $x_{n-2} \equiv (b_n + b_{n-1}) (\mathrm{mod}\ 2)$. Decreasing the indices of rows by 3, we sum these rows and the value of x_{n-2} and obtain the solution for x_{n-5}. Continuing this process, we obtain the second formula. At the same time, $\alpha \equiv 0 (\mathrm{mod}\ 3)$ cannot be true since, in this case, we have $n - 2 \equiv 0 (\mathrm{mod}\ 3)$ or $n \equiv -1 (\mathrm{mod}\ 3)$, contrary to the conditions of the theorem. The third formula is a consequence of the first two formulas if their values are substituted in the equation $x_{\alpha-1} + x_\alpha + x_{\alpha+1} = b_\alpha$. When $n \equiv 0 (\mathrm{mod}\ 3)$, the third formula is consistent but, when $n \equiv 1 (\mathrm{mod}\ 3)$, it contains the values $\alpha = 1$ and $\alpha = n$ for which fictitious variables x_0 and x_{n+1} equated to zero are added to the formula.

Theorem 4 does not give a definite answer concerning the value of $n \equiv -1 (\mathrm{mod}\ 3)$. In this case, as is obvious (Lemma 2), system (8) is linearly dependent. In order to obtain the solution, we eliminate the last equation and the variable x_n and assume that $b'_{n-1} = b_n + x_n$, which leads to the truth of the conditions of Theorem 4. After obtaining the solution of the changed system, we find b_n that satisfies condition (9) and then find $x_n = b_n + x_{n-1}$.

Let us consider one more undirected graph representing a cycle similar to the contour presented in Fig. 2. The system of equations (7) that specifies it also have rows each of which contains at least by one variable more than in similar system (6), i.e., we have

$$\left.\begin{array}{lllllll} x_1 + x_2 & . & . & . & + x_n & \equiv b_1 \\ x_1 + x_2 + x_3 & . & . & . & & \equiv b_2 \\ . \quad x_2 + x_3 + x_4 & . & . & & & \equiv b_3 \\ . \quad . \quad . & . & . & . & . & \\ x_1 + \ . \quad . & . & + x_{n-1} & + x_n & & \equiv b_n \end{array}\right\} \mathrm{mod}\ 2. \tag{11}$$

LEMMA 3. If the length of a cycle equals $n \equiv 0 (\mathrm{mod}\ 3)$, then the rank of the system of equations (11) for the cycle equals $n - 2$.

In fact, for such a system, we can derive the following equalities. If we add together the left sides of the equations with the numbers of rows 1, 4, 7, etc. with numbers $1 (\mathrm{mod}\ 3)$, then we obtain

$$\sum_{j=1}^{n} x_j = \sum_{i \equiv 1 (\mathrm{mod}\ 3)} b_i. \tag{12}$$

For other rows, we obtain similar equalities

$$\sum_{j=1}^{n} x_j = \sum_{i \equiv 2 (\mathrm{mod}\ 3)} b_i = \sum_{i \equiv 0 (\mathrm{mod}\ 3)} b_i. \tag{13}$$

From this we obtain the following two equalities with respect to the initial state of the safe:

$$\sum_{i=1}^{l} \left(b_{3i-1} + b_{3i-2} \right) = \sum_{i=1}^{l} \left(b_{3i} + b_{3i-1} \right) \equiv 0 (\mathrm{mod}\ 2), \tag{14}$$

where $l = n/3$.

We find b_{n-1} from the first equality and then, substituting it in the second equality, we find b_n as follows:

$$\begin{aligned} b_{n-1} &\equiv \left(\sum_{i=1}^{n-2} b_i + \sum_{i=1}^{l-1} b_{3i} \right) (\mathrm{mod}\ 2), \\ b_n &\equiv \left(\sum_{i=1}^{n-2} b_i + \sum_{i=1}^{l-1} b_{3i-1} \right) (\mathrm{mod}\ 2). \end{aligned} \tag{15}$$

If these conditions are not true, system (11) and, accordingly, the problem have no solution.

If we have $n \not\equiv 0 (\mathrm{mod}\ 3)$, then any sums in the left side of system (11) do not lead to equality (15). We denote by $R(i)$ the set of indices $\{i, i+1, i+3, i+4, \ldots, i+3j, i+3j+1\}$, where $1 \le i \le n$, $j = \left\lfloor \frac{n}{3} \right\rfloor$, and compute the mod n sums of the indices.

THEOREM 5. If we have $n \not\equiv 0 (\mathrm{mod}\ 3)$, then the problem on a safe formulated for a cycle of length n has the following solution:

$$x_\alpha \equiv \left(\sum_{i \in R(\alpha - \delta)} b_i + b_{\alpha - \delta} \right) (\mathrm{mod}\ 2), \quad 1 \le \alpha \le n, \tag{16}$$

where $\delta \equiv (n^2 + n + 1) (\mathrm{mod}\ 3)$.

Proof. We take the modulo mod 2 sum of the left sides of the equations of system (11) in which the indices of rows belong to the set $R(i)$. For the first pair, we have $(x_{i-1} + x_{i+1}) (\mathrm{mod}\ 2)$. Continuing the summution, we obtain $(x_{i-1} + x_{i+3j+2}) (\mathrm{mod}\ 2)$. If $n \equiv 1 (\mathrm{mod}\ 3)$, then we have $j = \left\lfloor \frac{n}{3} \right\rfloor = \frac{n-1}{3}$, and the sum equals $(x_{i-1} + x_{i+1}) (\mathrm{mod}\ 2)$. Adding the ith equation, we obtain x_i. Assuming that $\alpha = i$, we obtain formula (16) since we have $\delta \equiv 1 + 1 + 1 \equiv 0 (\mathrm{mod}\ 3)$. If $n \equiv -1 (\mathrm{mod}\ 3)$, then we have $j = \left\lfloor \frac{n}{3} \right\rfloor = \frac{n-2}{3}$, and the sum obtained above is equal to $(x_{i-1} + x_i) (\mathrm{mod}\ 2)$. Summing with the ith equation, we obtain x_{i+1}. Assuming that $\alpha = i + 1$, we obtain $x_\alpha \equiv \left(\sum_{i \in R(\alpha - 1)} b_i + b_{\alpha - 1} \right) (\mathrm{mod}\ 2)$, which also is consistent with the formula since we have $\delta \equiv (-1)^2 - 1 + 1 \equiv 1 (\mathrm{mod}\ 3)$. This completes the proof of the theorem.

For $n \equiv 0 (\mathrm{mod}\ 3)$, under conditions (15), we obtain the solution if we assign arbitrary values to x_{n-1} and x_n, transpose their values to the right sides of the equations with the numbers 1 and $n-2$, and eliminate the $(n-1)$th and nth equations. As a result, we obtain a system of equations for a chain of length $n \equiv 1 (\mathrm{mod}\ 3)$ that is solved for an arbitrary initial state of the safe.

Let us consider the example when $n = 9$ and $\mathbf{b} = (0, 1, 1, 0, 1, 0, 1, 1, 0)$. We compute $\sum_{i=1}^{n-2} b_i \equiv 0 + 1 + 1 + 0 + 1 + 0 + 1 \equiv 0 (\mathrm{mod}\, 2)$. Let us check conditions (15) as follows:

$1 = b_7 \equiv 0 + b_3 + b_6 \equiv 1$ (it is true);

$0 = b_8 \equiv 0 + b_2 + b_5 \equiv 0$ (it is true).

We assume that $x_7 = x_8 = 0$. As a result, we obtain the following system for a chain of length 7:

$$\left.\begin{array}{rcl} x_1 + x_2 \quad . \quad . \quad . \quad . \quad . & \equiv & 0 \\ x_1 + x_2 + x_3 \quad . \quad . \quad . \quad . & \equiv & 1 \\ . \quad x_2 + x_3 + x_4 \quad . \quad . \quad . & \equiv & 1 \\ . \quad . \quad x_3 + x_4 + x_5 \quad . \quad . & \equiv & 0 \\ . \quad . \quad . \quad x_4 + x_5 + x_6 \quad . & \equiv & 1 \\ . \quad . \quad . \quad . \quad x_5 + x_6 + x_7 & \equiv & 0 \\ . \quad . \quad . \quad . \quad . \quad x_6 + x_7 & \equiv & 1 \end{array}\right\} \mathrm{mod}\, 2. \qquad (17)$$

The solution of this system is as follows: $x_1 = x_2 = 0$, $x_3 = 1$, $x_4 = 0$, $x_5 = 1$, $x_6 = 0$, and $x_7 = 1$. Let us check the solution with the help of the corresponding switchings (the necessary switchings are underlined),

$\mathbf{b} = (0, 1, \underline{1}, 0, 1, 0, 1, 1, 0) \to (0, 0, 0, 1, \underline{1}, 0, 1, 1, 0)$

$\to (0, 0, 0, 0, 0, 1, \underline{1}, 1, 0) \to (0, 0, 0, 0, 0, 0, 0, 0, 0) = \mathbf{b}_{\mathrm{fin}}$.

CONCLUSIONS

The problem on a mathematical safe arose from some computer games. In the form of a concrete separate problem, it was described in [2], where the solution was obtained owing to implicit techniques. A more general approach was proposed in [3], where safes had a more complicated matrix form. In the latter work, the general solution of the problem on a safe defined on an arbitrary (0,1) matrix was also proposed. The problem becomes excessively complicated if it is defined on matrices specified on the set of states in a class of residues with an arbitrary modulus. In principle, such problems can be solved as systems of linear Diophantine equations and, to this end, one can use well-known methods [5]. However, the specificity of the problem on a mathematical safe allows one to create unique direct methods of solution. (We will consider them in subsequent publications.)

REFERENCES

1. G. A. Donets, "Solution of one problem on a safe," in: Intern. Conf. on Applied Mathematics Dedicated to the 65th Anniversary of B. N. Pshenichnyi (June 25–28, 2000), Kyiv (2000), p. 39.
2. A. P. Ventura, "How to turn all the lights out," Elem. Math., **55**, 135–141 (2000).
3. T. R. Walsh, "Cracking Saferacker," J. Recreat. Math., **17**, No. 4, 117–128 (1984–1985).
4. G. A. Donets "Solution of the safe problem on (0,1)-matrices," Kibern. Sist. Anal., No. 1, 98–105 (2002).
5. S. L. Kryvyi, "Methods of solution and criteria of compatibility of systems of linear Diophantine equations over the set of natural numbers," Kibern. Sist. Anal., No. 4, 12–36 (1999).